March 30, 2004

Statement for the Record of
Dan Verton
Senior Writer, Computerworld Magazine
Author, Black Ice: The Invisible Threat of Cyber-Terrorism (McGraw-Hill/Osborne, 2003)

On
Security and Telecommunications of Industrial Control Systems in our Nation's Critical Infrastructure

Before the
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census
House of Representatives Committee on Government Reform
Washington, D.C.

Good afternoon Chairman Putnam, Ranking Member Clay and Members of the Subcommittee.

I want to thank you and your staff for the honor of appearing before you today to discuss what I believe is an urgent national security matter and I applaud your leadership in this area.

At the outset, let me say that I appear before you today as somebody with no vested corporate interest in the outcome of this hearing and as an independent researcher whose statement and answers stem from years of confidential discussions with well-informed sources in the national security arena. Although I do not consider myself a technical expert in the control systems used in many of our nation's most critical industrial settings, I have a professional background in intelligence and information security, and I'm the author of a newly published book by McGraw-Hill titled *Black Ice: The Invisible Threat of Cyber-Terrorism* that goes into detail regarding the subject of today's hearing and that has been endorsed by some of the nation's leading authorities in critical infrastructure protection, terrorism and information security, including the president's two former chief cyber security advisors, Richard Clarke and Howard Schmidt.

Supervisory Control and Data Acquisition systems, or SCADA systems, are in many ways the crown jewels of some of the nation's most important industrial control settings, such as the electric power grid. But they are not – as their name might imply – built upon secret, proprietary technology. To the contrary, modern design specifications for SCADA systems, which I have documented through both personal interviews with experts and

through open-source research on the Internet, presents us with the frightening reality that the SCADA systems being used in our nation's critical infrastructures are nothing more than high-end commercial PCs and Servers running Microsoft Corp. operating systems. In other words, the genie is out of the bottle and has been for years in terms of understanding how to disrupt or corrupt the operations of SCADA systems. Today, it's simply a matter of gaining access. And as I have also documented in my research, gaining access to SCADA systems for the purpose of causing widespread chaos, confusion and economic damage is increasingly becoming a mere formality for professional hackers, virus and worm writers, and terrorist-sponsored saboteurs.

However, before I get to the critical issue of open access to SCADA systems and the vulnerability that they now increasingly face, let me say a brief word about the critical national security implications of this growing problem. Despite the impact of the Slammer worm and possibly the Blaster worm on the electric power industry – a primary user of SCADA systems for management and control of the electric grid -- the problem facing us today extends far beyond the electric power industry. While the electric power grid can be considered the first Domino in a cascading failure of critical infrastructures, SCADA systems are critical to the day-to-day and minute-to-minute operation of the natural gas pipeline system, chemical processing facilities, telecommunications networks, as well as municipal water and wastewater systems to name just a few. And while all of these sectors differ in terms of their level of modernization, all share a common modernization approach, which is based primarily around Web-based and wireless technologies for cost-savings and ease of management. And that brings me back to the issue of access to SCADA systems and their potential vulnerability.

We know for a fact that the forces of deregulation have given rise to an increasing number of deliberate and inadvertent connections between SCADA systems in the electric industry and the Internet-based corporate networks that utilities use to manage the business of buying and selling power. In fact, the integration and interoperability of SCADA systems with corporate IT systems is, in some cases, institutionalized as part of the IT contracting and acquisition process at some utility companies. For example, companies often require SCADA systems to be interoperable with corporate architectures (e.g., must be Windows 2000 and use the following password and logon structure . . .) before the systems can be purchased. All of these connections provide avenues of attack for hackers and terrorists online and also expand the universe of the so-called "trusted insider." All of this is of particular concern when you factor in statistics that indicate the average large utility company deals with about 1 million cyber security incidents per year that require some sort of investigation or response.

The energy industry has acknowledged the existence of these linkages and the imperative of protecting SCADA systems from unauthorized access. In December 2001, for example, the American Gas Association and the Gas Technology Institute met in Washington, D.C., to discuss the need for improved encryption to protect SCADA communications between key nodes in the natural gas grid. One of the slides used during the two days of presentations highlights the threats posed to SCADA communications from the use of commercial computer equipment, open communication protocols that are

widely published and available to anybody, linkages and reliance on the public switched telephone network, and the ability to steal the hardware.

In addition, a recent network architecture plan released by a major company in the water and wastewater industry included the following requirements for its SCADA systems: Peer-to-peer networking over TCP/IP (Transmission Control Protocol/ Internet Protocol—in other words, the Internet); software changes that can be downloaded from any node on the network; dial-in capabilities to all software functions; and a link to the existing pump station.

Consider the following additional examples, which I document in my book, Black Ice; The Invisible Threat of Cyber-Terrorism:

The U.S. railroad system's increasing use of wireless technologies may present one of the most immediate dangers to both national security and local safety. Given the system's long, winding network of radio, telephone, and computer assets, voice and data communications networks provide vital links between train crews, trackside monitoring and repair staff, and rail control centers. Total control of the massive network is accomplished through a communication system that integrates trackside maintenance telephones, trackside transponders, security cameras and monitors, passenger information displays, public announcements, the public telephone network, radio bases, and control center consoles. However, wireless SCADA systems are increasingly providing the management glue that keeps all of these systems running together. In the colder regions of the country, underground heaters keep the rails from freezing in winter. These operations are also being controlled and monitored by wireless SCADA computers. The use of modern technology in this case means that in the case of a failure, railroads no longer have to dispatch technicians in the dead of winter to remote locations where heating switches are usually located. However, it also means that the security of these switching operations may now have a new series of security challenges to deal with. This is of particular concern given the dangerous nature of some train cargo.

The City of Brighton, Michigan, is one example. Brighton is a city of only 6,500. But that population skyrockets to more than 70,000 each day due to a thriving business district and a boom in hotel space. However, beneath the streets of Brighton is a **water and wastewater system** that is controlled in part by wireless technology. The remote terminals monitor pump run time, pump failures, flood sensors, high water level alarms, and power, as well as site intrusion alarms and manually activated panic buttons. The utility also planned to equip work vehicles with a controller connected to a laptop computer. "With critical data now available at just the click of a mouse, the laborious, time-consuming, and often hazardous, need for utility workers to make daily rounds to check pump status at each of the lift stations is a thing of the past," claimed marketing material from one of the contractors responsible for installing the equipment. The mobile controller would then allow utility engineers to monitor the waste water system while they're driving around the city.

Uranium mining operations in Wyoming extract uranium from the soil through a process by which water is injected into the ground. Because of the contamination, remote terminals are necessary to control and manage the pumps that move the water and extract the uranium. Commercial PC-based remote workstations now support critical monitoring functions, such as pump failure, pump status, temperature, speed, and even the pump's on/off condition. But the security implications are enormous. When pumps lose power, water pressure starts building up in

the plant. Software has been programmed to automatically reset certain pumps to get the pressure out as fast as possible. And it's all being done in the name of cost-effectiveness.

In states throughout the **Midwest, one can find oil wells** arranged in a twelve-mile-diameter circle. They are part of what's known in the vernacular of the oil industry as a **"water flood" operation**. However, with such a large number of pumps and holding tanks to manage, drilling companies are increasingly turning their attention to wireless SCADA systems to monitor critical functions of the operation, including emergency systems that are designed to ensure environmental safety. For example, wireless SCADA systems are used to monitor pressure and flow rates in both oil and water pipelines. When flow rates drop below normal levels, the system is designed to turn on additional pumps. In addition, if pipeline pressure or tank levels exceed normal operating limits the system will turn various pumps off. They are also used to monitor tank levels and overflow pit levels —a critical safety indicator that could have environmental consequences if it fails. And as in the case of the 911 emergency systems, oil well managers and technicians also have remote dial-in connection capabilities.

Mr. Chairman, let me conclude with a final word about how we must think about these vulnerabilities in post-Sept. 11 America.

The pervasive intellectual rigidity that surrounds the issue of cyber-terrorism has created two competing camps of thought. One camp, consisting mostly of individuals with years of formal training and experience in national security from a holistic point of view (i.e., the relationship between physical security and cybersecurity, and the adaptive nature of international terrorism), accepts the notion that America is facing a thinking enemy that is far more capable than most people are willing to accept. The other camp, consisting mainly of self-proclaimed experts, industry "analysts," and Internet security professionals whose expertise is limited significantly to the virtual realm of the computer, remains the last, fading bastion of hope for those who want desperately to hang on to the conception of traditional "physical" terrorism as the only legitimate form of terrorism. This latter group falls into the same category as those who, prior to September 11, 2001, considered airborne threats to physical infrastructure too bizarre to spend time and resources preparing for.

Since the start of the U.S. War on Terrorism, a significant amount of evidence has been unearthed throughout Afghanistan and various other al-Qaeda hideouts around the world that indicates terrorism may be evolving toward a more high-tech future at a faster rate than previously believed. In January 2002, for example, U.S. forces in Kabul discovered a computer at an al-Qaeda office that contained models of a dam, made with structural architecture and engineering software. The software would have enabled al-Qaeda to study the best way to attack the dam and to simulate the dam's catastrophic failure. In addition, al-Qaeda operatives apprehended around the world acknowledged receiving training in how to attack key infrastructures. Among the data terrorists were studying was information on SCADA systems.

For the most part, these dire warnings have gone unheeded by the private- sector companies that own and operate these infrastructure systems. Senior executives view such scenarios as something akin to a Hollywood movie script. However, throughout the entire post-September 11 security review process, a process that continues to this day,

administration experts and other senior members of the U.S. intelligence community were quietly coming to the conclusion that they were witnessing the birth of a new era of terrorism. Cyberspace, with its vast invisible linkages and critical role in keeping America's vital infrastructures and economy functioning, was fast becoming a primary target and a weapon of terror.

Mr. Chairman, my fear is that the next time we have a massive power failure, such as we experienced on Aug. 14, it will not be a self-inflicted wound, but potentially a terrorist-induced failure that is quickly exploited by suicide bombings, rampaging gunmen or chemical and biological attacks against those stranded in the subway systems. Real-world, cross-border exercises between the U.S. and Canada, including one from which the title of my book is taken, have already shown that physical and cyber attacks can cause cascading failures throughout multiple regional infrastructures, including power outages that could last for several months. And these exercises were written and war-gamed by the actual owners and operators of critical infrastructures based on a self-assessment of their own worst fears and worst-case scenarios. After action reports indicate that infrastructure owners have at best a surface-level understanding of the interdependent nature of their infrastructures and few know exactly how to prevent such failures from spreading out of control.

My recommendations to the Subcommittee are as follows:

1. Require background investigations or security clearances for private sector workers with direct access to SCADA systems, control centers or communications facilities that operate our nation's most critical infrastructures. This is a national security issue and it should be treated as such.
2. Red Team the infrastructure immediately and independently. It is time for "Eligible Receiver II." The government should develop, sponsor and conduct a "no-notice" Red Team assessment of the nation's critical infrastructures to determine the true level of security and preparedness.
3. Push the "market" into action, because the market will not and has not volunteered to be the defender of America in this age of Internet-enabled threats. This will require a mix of new regulations coupled with insurance industry action to offer premiums that are responsive to government-certified security audits. This is not heavy-handed government regulation, it is leadership in the form of "Trust, but verify."
4. Sponsor a more aggressive research & development program in SCADA system security devices and software. The genie is out of the bottle. The international demonstration effect of Aug. 14 cannot be denied.
5. Congress should provide strict oversight of the energy industry's $100 billion upgrade program for the next generation power grid to ensure that security is the first priority. Separate networks, similar to the failed GovNet initiative, should not be taken off the table.

I thank you for this opportunity to share with you some of my research and opinions on this matter. I would be happy to answer your questions.

Additional Resources:

Blaster Worm Linked to Severity of Blackout
http://www.computerworld.com/databasetopics/data/story/0,10801,84519,00.html

CIOs, Experts Cite Urgent Need for U.S. Infrastructure Upgrade
Some energy CIOs and experts said similar or worse failures are possible in the future if the industry and government fails to develop more modern control systems.
http://www.computerworld.com/industrytopics/energy/story/0,10801,84096,00.html

Black Ice
In his new book, Black Ice, Computerworld's Dan Verton says the private sector is in a state of denial about the serious threat of cyber-terrorism against power plants, telecom sites and other critical facilities.
http://www.computerworld.com/industrytopics/energy/story/0,10801,83841,00.html

Utility Companies Face Barrage of Cyberattacks
Many utility companies, which own and operate critical power networks, are finding it more and more difficult to keep up with the number of cybersecurity incidents involving their control systems, according to experts who attended a conference last week in New Orleans.
http://www.computerworld.com/industrytopics/energy/story/0,10801,67581,00.html

Movement afoot to beef up industrial cybersecurity
Efforts to boost IT security for major industrial-control systems that are critical to infrastructure protection are picking up steam.
http://www.computerworld.com/industrytopics/energy/story/0,10801,70587,00.html

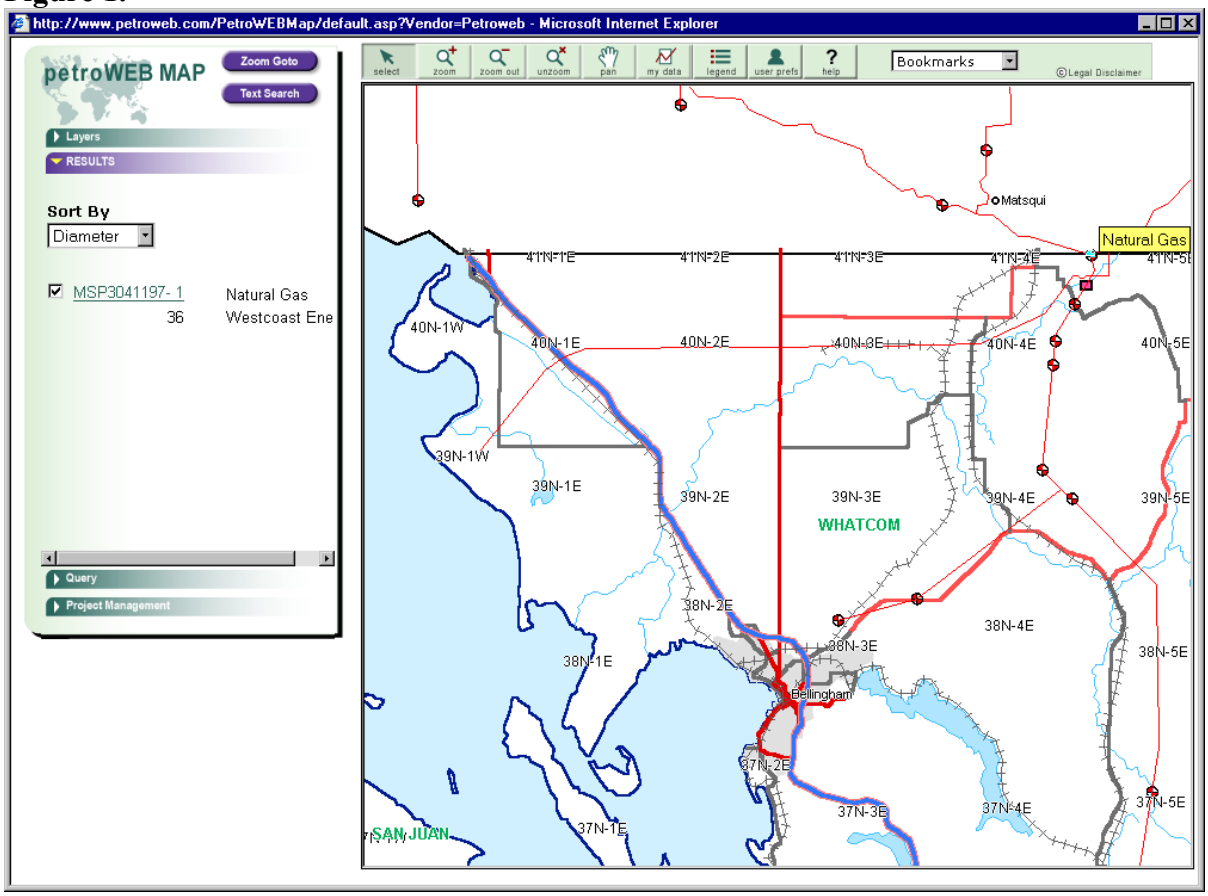
California Hack Points to Possible Surveillance Threat
The revelation that hackers broke into computer systems owned by California's primary electric power grid operator and remained undetected for 17 days this spring highlights a growing fear on the part of federal officials that such intrusions could be part of long-term intelligence-gathering activities.
http://www.computerworld.com/industrytopics/energy/story/0,10801,61432,00.html

Sept. 11 lessons drive key aspects of Bush cyberdefense plan
Physical security, industrial control systems and tests of federal IT security are all featured prominently in the national strategy unveiled yesterday.
http://www.computerworld.com/governmenttopics/government/story/0,10801,74359,00.html

Energy: The First Domino in Critical Infrastructure
More research and development is needed to protect critical industrial systems in the energy sector against cyberattack, officials say.
http://www.computerworld.com/securitytopics/security/story/0,10801,74077,00.html

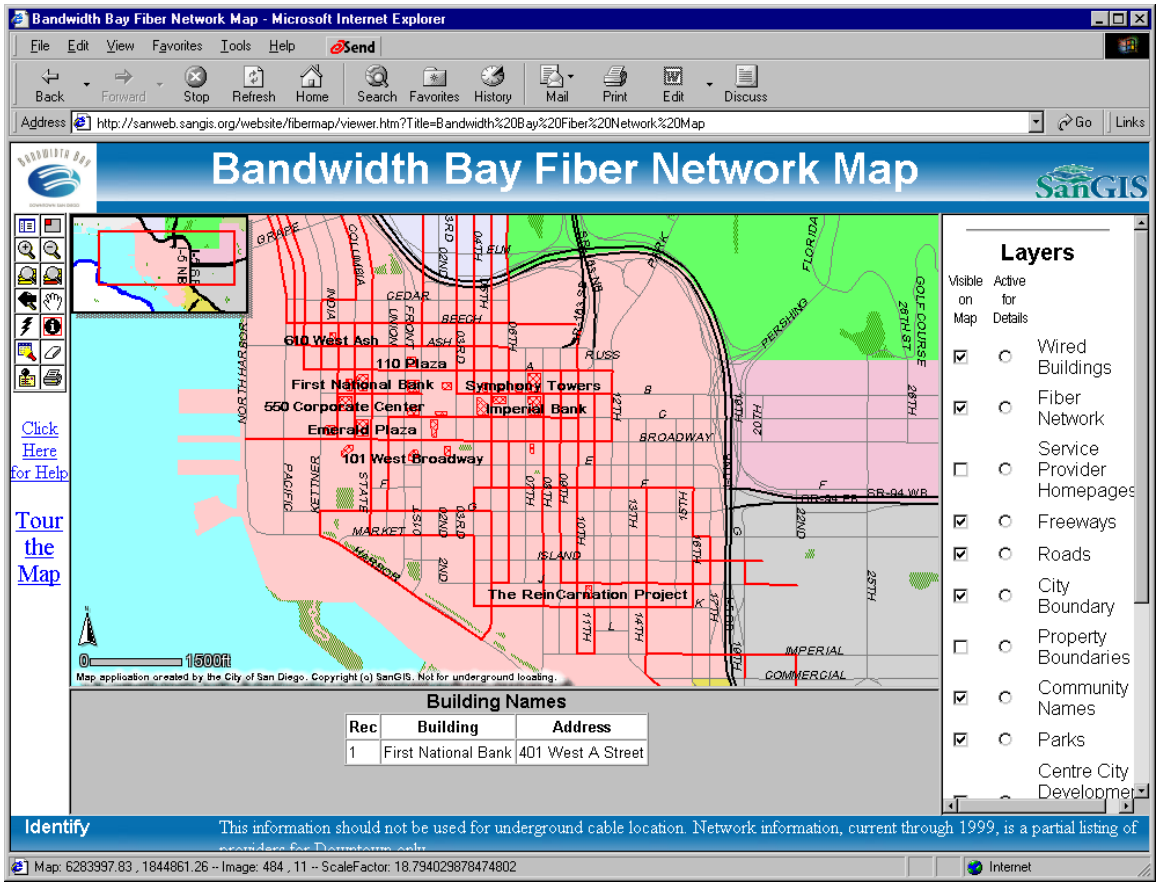
The Genie Is Out of the Bottle

Figure 1.



This is a photo taken from a publicly available Web site that depicts the most sensitive natural gas pipeline interconnection point in the U.S. What's interesting about this Web page is that it is completely interactive, not only allowing the user to zoom into great detail, but also providing latitude and longitude coordinates and detailed terrain/man-made landmarks.

Figure 2



Detailed, street-level maps of metropolitan area fiber networks are also available online, and include building and company names through which these high-speed interconnections pass.

Other Sensitive Data Available on Government & Corporate Web Sites

1. Detailed maps depicting the termination points along the entire Eastern Seaboard for all long-haul undersea fiber lines.
2. Maps depicting the storage locations of all spent nuclear fuel waste in the U.S.
3. Telecommunications network maps from which the location of current and planned critical facilities and nodes can be derived.
4. One telecom company offered location information for all of the company's five data centers, as well as a virtual tour inside a "typical" center, including a description of all security systems used to protect the facility.
5. Detailed descriptions by IT companies of deployment case studies involving SCADA systems.
6. Load-bearing capacities of elevators in large office buildings as well as location of ventilation and air conditioning systems.
7. Number of people employed at certain office buildings as well as maps and interactive photos of building and facility layout.